Arch. Math. 101 (2013), 213–218

0003-889X/13/030213-6
published online September 11, 2013
DOI 10.1007/s00013-013-0551-y

Archiv der Mathematik

On certain biquadratic equations

A. Schinzel and M. Skałba

Abstract. It is proved that if certain biquadratic equations with a prime parameter and four unknowns have a non-trivial solution in the integers, then they have infinitely many such solutions.

Keywords. Pell equation, Biquadratic Diophantine equation, Cyclotomic polynomial.

The diophantine equation $f(x, y, z, t) = c$, where f is a quartic form and $c \neq 0$, has been studied only in the case where f splits over the complex field. The aim of this paper is to prove the following theorems.

Theorem 1. *If $p \equiv 3 \pmod 4$ is a prime , $\alpha \equiv 1 \pmod 2$, $D = p^\alpha$, and the equation $(x^2 + y^2)^2 - D(z^2 + t^2)^2 = 1$ has at least one integer solution with $z^2 + t^2 > 0$, then it has infinitely many integer solutions.*

Theorem 2. *If $p \equiv 3 \pmod 8$ is a prime , $\alpha \equiv 1 \pmod 2$, $D = p^\alpha$, and the equation $(x^2 + y^2)^2 - D(z^2 + t^2)^2 = -2$ has at least one integer solution, then it has infinitely many.*

Theorem 3. *If $p \equiv 7 \pmod 8$ is a prime , $\alpha \equiv 1 \pmod 2$, $D = p^\alpha$, and the equation $(x^2 + y^2)^2 - D(z^2 + t^2)^2 = 2$ has at least one integer solution, then it has infinitely many.*

It is natural to ask about the number $N_i(x)$ of values $D < x$ covered by the above Theorem i $(i = 1, 2, 3)$. We cannot prove that $\lim_{x\to\infty} N_i(x) = \infty$, but since Theorem 2 and 3 apply to all odd primes of the form $(x^2 + y^2)^2 \pm 2$ and Theorem 1 applies to all odd primes of the form $(x^2 + y^2)^2 + 2$ at least heuristically $N_i(x) \gg \frac{x^{1/2}}{(\log x)^{3/2}}$ $(i = 1, 2, 3)$. The method does not seem applicable to other equations $(x^2 + y^2)^2 - D(z^2 + t^2)^2 = c$, where $c \neq 0$.

Lemma 1. *Let n be an odd, square-free integer > 3 and $\Phi_n(x)$ the n-th cyclotomic polynomial. Then $\Phi_n(z)$ can be written in the form*

$$4\Phi_n(z) = A_n(z)^2 - (-1)^{(n-1)/2} n z^2 B_n(z)^2,$$

where $A_n(z)$ and $B_n(z)$ have integer coefficients and are of degree $\phi(n)/2$ and $\phi(n)/2-2$, respectively. $A_n(z)$ is symmetric if its degree is even, otherwise it is anti-symmetric. $B_n(z)$ is symmetric for n prime.

Proof. See [[1], p.330 and 445]. □

Lemma 2. *For $p \equiv 3 \pmod 4$ a prime, $p > 3$, $A_p(z)$ is divisible by $z-1$ and $B_p(z)$ is divisible by $z+1$.*

Proof. We have [[1], p.330] □

$$A_p(z) + \sqrt{-p}B_p(z) = 2\prod_{(\frac{r}{p})=1}(z-\zeta_p^r),$$

$$A_p(z) - \sqrt{-p}B_p(z) = 2\prod_{(\frac{s}{p})=-1}(z-\zeta_p^s).$$

If $p \equiv 3 \pmod 4$ is a prime, then $(\frac{r}{p}) = 1$ is equivalent to $(\frac{-r}{p}) = -1$. Since for $p > 3$, $\sum_{(\frac{r}{p})=1} r \equiv 0 \pmod p$, we obtain

$$\prod_{(\frac{s}{p})=-1}(1-\zeta_p^s) = \prod_{(\frac{r}{p})=1}(1-\zeta_p^{-r}) = -\prod_{(\frac{r}{p})=1}(1-\zeta_p^r);$$

$$\prod_{(\frac{s}{p})=-1}(-1-\zeta_p^s) = \prod_{(\frac{r}{p})=1}(-1-\zeta_p^{-r}) = \prod_{(\frac{r}{p})=1}(1-\zeta_p^r),$$

thus $A_p(1) = B_p(-1) = 0$ and the lemma follows.

Lemma 3. *If a form $F \in \mathbb{Q}[x,y]$ satisfies $F(x,y) = F(y,x)$ and $d := \deg F \equiv 0 \pmod 2$, then $F = G((x+y)^2, xy)$, where $G \in \mathbb{Q}[z,t]$.*

Proof. By the theorem on symmetric functions $F = H(x+y, xy)$, where $H \in \mathbb{Q}[z,t]$. Let $F(x,y) = \sum a_{\alpha\beta}(x+y)^\alpha(xy)^\beta$. Since for $a_{\alpha\beta} \neq 0$ we have $\alpha+2\beta = d \equiv 0 \pmod 2$, we have $a_{\alpha\beta} = 0$ for α odd. □

Lemma 4. *Let $D = p^\alpha$, where $p \equiv 3 \pmod 4$ is a prime, $\alpha \equiv 1 \pmod 2$, and positive integers u, v satisfy $u^2 - Dv^2 = 1$. Put*

$$\xi = u + v\sqrt{D}, \xi^{-1} = u - v\sqrt{D}; L_n = \frac{\xi^n - \xi^{-n}}{\xi - \xi^{-1}}, \tag{1}$$

and

$$E_n = \frac{\xi^n + \xi^{-n}}{2}, F_n = vL_n. \tag{2}$$

E_n and F_n are positive integers satisfying

$$E_n^2 - DF_n^2 = 1. \tag{3}$$

Moreover, for all positive integers n,

$$E_{p^n}/E_{p^{n-1}} \text{ is a sum of two squares.} \tag{4}$$

Proof. We have

$$E_n^2 - DF_n^2 = \frac{\xi^{2n} + 2 + \xi^{-2n}}{4} - Dv^2 \frac{\xi^{2n} - 2 + \xi^{-2n}}{4v^2 D} = 1,$$

which proves (3). Moreover,

$$E_{p^n}/E_{p^{n-1}} = \Phi_{2p^n}(\xi, \xi^{-1}) = \Phi_{2p}(\xi^{p^{n-1}}, \xi^{-p^{n-1}}) = \Phi_p(-\xi^{p^{n-1}}, \xi^{-p^{n-1}}), \quad (5)$$

where $\Phi_n(x, y)$ is a homogeneous form of $\Phi_n(z)$. By Lemma 1 for $p > 3$

$$4\Phi_p(-\xi^{p^{n-1}}, \xi^{-p^{n-1}}) = A_p(-\xi^{p^{n-1}}, \xi^{-p^{n-1}})^2 + pB_p(-\xi^{p^{n-1}}, \xi^{-p^{n-1}})^2. \quad (6)$$

Since A_p is anti-symmetric, $A_p(-\xi^{p^{n-1}}, \xi^{-p^{n-1}})$ is symmetric in ξ, ξ^{-1}, hence is an integer. Now $B_p(x, y)$ is, by Lemma 2, divisible by $x+y$, and the quotient is of degree $\frac{p-1}{2} - 3 \equiv 0 \pmod 2$. By Lemma 3 the quotient is a polynomial in $(x + y)^2$ and xy. It follows that $B_p(-\xi^{p^{n-1}}, \xi^{-p^{n-1}})^2 = pw^2$ with $w \in \mathbb{Q}$.

(4) follows now from (5) and (6). It remains to consider $p = 3$. Let $\xi^{3^{n-1}} = u_n + v_n\sqrt{3^\alpha}$. We have by (5)

$$\begin{aligned} E_{3^n}/E_{3^{n-1}} &= \Phi_3(-\xi^{3^{n-1}}, \xi^{-3^{n-1}}) \\ &= (u_n + v_n\sqrt{3^\alpha})^2 - (u_n + v_n\sqrt{3^\alpha})(u_n - v_n\sqrt{3^\alpha}) + (u_n - v_n\sqrt{3^\alpha})^2 \\ &= u_n^2 + (3^{\frac{\alpha+1}{2}} v_n)^2. \end{aligned}$$

□

Lemma 5. *In the notation of Lemma 4,*

$$F_{p^n}/pF_{p^{n-1}} \text{ is a sum of two squares.} \quad (7)$$

Proof We have by (1) and (2)

$$F_{p^n}/F_{p^{n-1}} = \Phi_{p^n}(\xi, \xi^{-1}) = \Phi_p(\xi^{p^{n-1}}, \xi^{-p^{n-1}}) \quad (8)$$

and by Lemma 1,

$$4F_{p^n}/F_{p^{n-1}} = A_p(\xi^{p^{n-1}}, \xi^{-p^{n-1}})^2 + pB_p(\xi^{p^{n-1}}, \xi^{-p^{n-1}})^2. \quad (9)$$

Since $A_p(x, y)$ is anti-symmetric, $A_p(x, y)/(x - y)$ is symmetric and

$$A_p(\xi^{p^{n-1}}, \xi^{-p^{n-1}})^2 = pw^2, w \in \mathbb{Q}. \quad (10)$$

Also $B_p(x, y)$ is symmetric, $B_p(\xi^{p^{n-1}}, \xi^{-p^{n-1}})$ is an integer, and (7) follows from (9) and (10). It remains to consider $p = 3$. Let again $\xi^{3^{n-1}} = u_n + v_n\sqrt{3^\alpha}$. We have by (8)

$$\begin{aligned} F_{3^n}/3F_{3^{n-1}} &= \frac{1}{3}\Big((u_n + v_n\sqrt{3^\alpha})^2 + (u_n + v_n\sqrt{3^\alpha})(u_n - v_n\sqrt{3^\alpha}) \\ &\quad + (u_n - v_n\sqrt{3^\alpha})^2\Big) \\ &= u_n^2 + (3^{\frac{\alpha-1}{2}} v_n)^2. \end{aligned}$$

Proof of Theorem 1. It follows by induction on n from Lemmas 4 and 5 that for n even E_{p^n} and F_{p^n} are sums of two squares. The formula (3) gives the theorem. □

Lemma 6. *Let $\varepsilon = \pm 1$, $D = p^\alpha$, where $p \equiv 5 + 2\varepsilon \pmod 8$ is a prime, $\alpha \equiv 1 \pmod 2$, and positive integers u, v satisfy $u^2 - Dv^2 = 2\varepsilon$. Put*

$$\eta = \frac{\sqrt{2\varepsilon}u + \sqrt{2D\varepsilon}v}{2}, \eta^{-1} = \frac{\sqrt{2\varepsilon}u - \sqrt{2D\varepsilon}v}{2}, P_n = \frac{\eta^n - \eta^{-n}}{\eta^{(n,2)} - \eta^{-(n,2)}}, \quad (11)$$

and

$$G_n = \frac{\eta^n + \eta^{-n}}{\sqrt{2\varepsilon}}, H_n = vP_n. \quad (12)$$

G_n and H_n are rational integers satisfying

$$G_n^2 - DH_n^2 = 2\varepsilon. \quad (13)$$

Moreover, for all positive integers n,

$$G_{p^n}/\varepsilon G_{p^{n-1}} \text{ is a sum of two squares.} \quad (14)$$

Proof. We have for odd n

$$G_n^2 - DH_n^2 = \frac{\eta^{2n} + 2 + \eta^{-2n}}{2\varepsilon} - Dv^2\frac{\eta^{2n} - 2 + \eta^{-2n}}{2\varepsilon Dv^2} = \frac{4}{2\varepsilon} = 2\varepsilon,$$

which proves (13). P_n as a Lehmer number is a rational integer, so is H_n and, by (13), G_n is an algebraic integer. However, it is also rational being invariant to all automorphisms of $\mathbb{Q}(\sqrt{2\varepsilon}, \sqrt{D})$. Moreover,

$$G_{p^n}/G_{p^{n-1}} = \Phi_{2p^n}(\eta, \eta^{-1}) = \Phi_{2p}(\eta^{p^{n-1}}, \eta^{-p^{n-1}}) = \Phi_p(-\eta^{p^{n-1}}, \eta^{-p^{n-1}}). \quad (15)$$

By Lemma 1 for $p > 3$

$$4\Phi_p(-\eta^{p^{n-1}}, \eta^{-p^{n-1}}) = A_p(-\eta^{p^{n-1}}, \eta^{-p^{n-1}})^2 + pB_p(-\eta^{p^{n-1}}, \eta^{-p^{n-1}})^2. \quad (16)$$

Since $A_p(x, y)$ is anti-symmetric, $A_p(-x, y)$ is symmetric and by Lemma 2, divisible by $x + y$. The quotient is of degree $\frac{p-1}{2} - 1 \equiv 0 \pmod 2$, hence, by Lemma 3, is a polynomial in $(x+y)^2$ and xy. It follows that $A_p(-\eta^{p^{n-1}}, \eta^{-p^{n-1}})^2 = 2\varepsilon w_1^2$, $w_1 \in \mathbb{Q}$. Again, by lemmas 2 and 3, $B_p(-\eta^{p^{n-1}}, \eta^{-p^{n-1}})^2 = 2\varepsilon p w_2^2$, $w_2 \in \mathbb{Q}$ and (14) follows by (15) and (16). It remains to consider $p = 3$. Let $\eta^{3^{n-1}} = \sqrt{2\varepsilon}u + \sqrt{2\varepsilon \cdot 3^\alpha}v$. Then

$$\begin{aligned}
&\Phi_3(-\eta^{3^{n-1}}, \eta^{-3^{n-1}}) \\
&\quad = (\sqrt{2\varepsilon}u + \sqrt{2\varepsilon \cdot 3^\alpha}v)^2 - (\sqrt{2\varepsilon}u + \sqrt{2\varepsilon \cdot 3^\alpha}v)(\sqrt{2\varepsilon}u - \sqrt{2\varepsilon \cdot 3^\alpha}v) \\
&\qquad + (\sqrt{2\varepsilon}u - \sqrt{2\varepsilon \cdot 3^\alpha}v)^2 \\
&\quad = 2\varepsilon(u^2 + (3^{\frac{\alpha+1}{2}}v)^2) = \varepsilon(u + 3^{\frac{\alpha+1}{2}}v)^2 + \varepsilon(u - 3^{\frac{\alpha+1}{2}}v)^2.
\end{aligned}$$

□

Lemma 7. *In the notation of Lemma 6, for all positive integers n,*

$$H_{p^n}/\varepsilon p H_{p^{n-1}} \text{ is a sum of two squares.} \quad (17)$$

Proof. We have by (11) and (12)

$$H_{p^n}/H_{p^{n-1}} = \Phi_{p^n}(\eta, \eta^{-1}) = \Phi_p(\eta^{p^{n-1}}, \eta^{-p^{n-1}}) \tag{18}$$

and by Lemma 1,

$$4H_{p^n}/H_{p^{n-1}} = A_p(\eta^{p^{n-1}}, \eta^{-p^{n-1}})^2 + pB_p(\eta^{p^{n-1}}, \eta^{-p^{n-1}})^2. \tag{19}$$

Since $A_p(x, y)$ is anti-symmetric, $A_p(x, y)/(x - y)$ is symmetric of even degree and, by Lemma 3,

$$A_p(\eta^{p^{n-1}}, \eta^{-p^{n-1}})^2 = 2\varepsilon p w_3^2, w_3 \in \mathbb{Q}. \tag{20}$$

Also $B_p(x, y)/(x + y)$ is symmetric of even degree, hence

$$B_p(\eta^{p^{n-1}}, \eta^{-p^{n-1}})^2 = 2\varepsilon w_4^2, w_4 \in \mathbb{Q}. \tag{21}$$

(17) follows from (18)–(21). It remains to consider $p = 3$. Let $\eta^{3^{n-1}} = \sqrt{2\varepsilon}u + \sqrt{2\varepsilon \cdot 3^\alpha}v$. Then

$$\begin{aligned} &F_{3^n}/3\varepsilon F_{3^{n-1}} \\ &\quad = \frac{1}{3\varepsilon}\Big((\sqrt{2\varepsilon}u + \sqrt{2\varepsilon \cdot 3^\alpha}v)^2 + (\sqrt{2\varepsilon}u + \sqrt{2\varepsilon \cdot 3^\alpha}v)(\sqrt{2\varepsilon}u - \sqrt{2\varepsilon \cdot 3^\alpha}v) \\ &\qquad + (\sqrt{2\varepsilon}u - \sqrt{2\varepsilon \cdot 3^\alpha}v)^2\Big) \\ &\quad = 2(u^2 + v^2) = (u + v)^2 + (u - v)^2. \end{aligned}$$

□

Proof of Theorem 2–3. It follows by induction on n from Lemmas 6 and 7 that for n even G_{p^n} and H_{p^n} are sums of two squares. The formula (13) gives the theorems. □

Reference

[1] H. Riesel, Prime Numbers and Computer Methods for Factorization, Birkhäuser 1985.

A. Schinzel
Institute of Mathematics,
Polish Academy of Sciences,
Sniadeckich 8,
P.O.Box 21,
00-956 Warszawa,
Poland
e-mail: schinzel@impan.gov.pl

M. Skałba
Institute of Mathematics,
University of Warsaw,
Banacha 2,
02-097 Warszawa,
Poland
e-mail: skalba@mimuw.edu.pl

Received: 22 April 2013